Notice of Allowability	Application No.	Applicant(s)	
	09/759,127	KURSAWE ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment filed on March 8, 2005*.

2. ☒ The allowed claim(s) is/are *23*.

3. ☒ The drawings filed on *21 January 2001* are accepted by the Examiner.

4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☒ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: *all, see attachment*.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

6/1/05

RD

NOTICE OF ALLOWANCE

Priority

1. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in the European Patent Office on January 14, 2000. It is noted, however, that applicant has not filed a certified copy of the foreign application 00100723.6 as required by 35 U.S.C. 119(b).

The applicant is directed to the MPEP, section 37 CFR 1.55.

Claim for foreign priority.
(a)(2) The claim for priority and the certified copy of the foreign application specified in 35 U.S.C. 119(b) or PCT Rule 17 must, in any event, be filed before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by the processing fee set forth in § 1.17(i), but the patent will not include the priority claim unless corrected by a certificate of correction under 35 U.S.C. 255 and § 1.323

B. Certification of the Priority Papers
35 U.S.C. 119(b)(3) authorizes the Office to require the applicant to furnish a certified copy of priority papers. Applicants are required to submit the certified copy of the foreign application specified in 35 U.S.C. 119(b) or PCT Rule 17 before the patent is granted. If the claim for priority or the certified copy of the foreign application is filed after the date the issue fee is paid, it must be accompanied by the processing fee set forth in 37 CFR 1.17(i), but the patent will not include the priority claim unless corrected by a certificate of correction under 35 U.S.C. 255 and 37 CFR 1.323. See 37 CFR 1.55(a)(2).

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance:

As per independent claims 1 and 19, it was not found to be taught in the prior art of broadcasting a share value to participating network devices to generate an

unpredictable bit, receiving *k* share values from the participating network devices, where *k* is larger than *t*, t being a number of faulty devices, and assembling out of those a common value and a deriving bit.

As per independent claims 2 and 20, it was not found to be taught in the prior art of broadcasting to all participating network devices a share value to open a cryptographic common coin and receiving k share values wherein k is larger than t, t being a number of faulty devices, and assembling out of those a common value and uncovering a bit out of the common value.

As per independent claim 21, it was not found to be taught in the prior art of broadcasting to the participating network devices a share value and assembling a common value by a combination of at least two share values in the exponent of the common number and uncovering a binary value of the common value.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Cachin, US 2004/0254967 discloses of the Byzantine Agreement protocol using randomization that utilizes common coin protocols.

Dellow et al, US 2004/0156507 discloses of decrypting broadcasted signals by utilizing a common key from a common key store.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

CR
June 1, 2005

6/1/05